REMOTE ACCESS CONTROL FEATURE FOR LIMITING ACCESS TO CONFIGURATION FILE COMPONENTS

FIELD OF THE INVENTION

The present invention generally relates to network communications and, more particularly, to a method and system for customizing a broadband access device configuration file to provide security for a service provider and/or service features for the end user.

BACKGROUND OF THE INVENTION

On many Broadband Access Products such as a Data Over Cable Service Interface Specification (DOCSIS) Cable Modem, valuable troubleshooting diagnostic information elements are made available to the end user by means of an HTTP server built into the device. This built-in server enables the end user to view, using a personal computer, web pages containing this diagnostic information. However, Service Providers who purchase and/or deploy these products vary greatly in their policies as to exactly what information elements they feel can be revealed to end users without compromising their companies' internal service security standards.

Therefore, a need exists for a feature, which enables the Service Provider to, from their location, remotely configure an in-home device to reveal information elements needed to provide a service or protect the service provider's system, but still limit access to additional information.

SUMMARY OF THE INVENTION

A security system for use in a distributed network includes a service provider selectively accessible via a network by a plurality of end users each having an access device for accessing the network. A control mechanism is included which is disposed at a location of the service provider and accesses and modifies stored information on each access device of the end users to designate portions of the information to prevent access thereof by the end users.

BRIEF DESCRIPTION OF THE DRAWINGS

The advantages, nature, and various additional features of the invention will appear more fully upon consideration of the illustrative embodiments now to be described in detail in connection with accompanying drawings wherein:

FIG. 1 is an exemplary block/system diagram showing network access devices connected to a network via service provider having a control mechanism for limiting access to the network access devices by an end user in accordance with the present invention;

FIG. 2 is a block/system diagram showing information categories for the network access devices in accordance with one embodiment of the present invention; and

FIG. 3 is a block/flow diagram showing an illustrative method for maintaining system security for a network service provider in accordance with the present invention.

It should be understood that the drawings are for purposes of illustrating the concepts of the invention and are not necessarily the only possible configuration for illustrating the invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides a method and system for remotely configuring a broadband access device to provide or maintain the service provider's system security. The present invention may also provide configurable diagnostic tools or other services, which are provided and configured remotely by the service provider.

In one embodiment, a distributed software control mechanism is provided by which a Broadband Access Service Provider (e.g., cable operator) can specify exactly which, if any, elemental diagnostic information will be available to the end user of the access device. This may be performed by including elements in a Broadband Access Device configuration file, which is preferably downloaded during the device startup. The needed software may be distributed between the configuration file (configuration instructions) and the access device (firmware).

It is to be understood that the present invention is described in terms of a cable access system; however, the present invention is much broader and may include any distributed system, which is maintained and serviced by a service provider. In addition, the present invention is applicable to any system including telephone networks, set top box access systems, computer networks, satellite networks, Internet systems, etc. The present invention is described in terms of a cable network; however, the concepts of the present invention may be extended to DSL, wireless or other network types using other technologies.

It should also be understood that the elements shown in the FIGS. may be implemented in various forms of hardware, software or combinations thereof. Preferably, these elements are implemented in a combination of hardware and software on one or more appropriately programmed general-purpose devices, which may include a processor, memory and input/output interfaces.

Referring now in specific detail to the drawings in which like reference numerals identify similar or identical elements throughout the several views, and initially to FIG. 1, a system architecture 10 for distributing voice, data and/or video information is shown. System architecture 10 is presented in an exemplary cable or Internet environment for employing the inventive method and system. However, the system may be employed in a plurality of other applications including wireless or satellite networks, local area networks, etc. Details of the individual block components making up the system architecture which are known to skilled artisans will only be described in details sufficient for an understanding of the present invention. The system block diagram 10 is composed of several functional blocks.

A service provider 100 provides services to end users 95 with access devices 102. Access devices 102 are employed as an interface between a network 101 (such as the Internet, cable network, etc.) and end user's equipment that may include a personal computer 110 (FIG. 2) or other device or system. When access device 102 is initially set up, information is downloaded from service provider 100, which is used to configure access device 102. This enables access device 102 to establish communication through the service provider 100 to network 101.

Each access device 102 preferably includes a configuration file 104 which stores web addresses and other configuration information that permits access device 102 to connect with network 101 through service provider 100. In

accordance with the present invention, service provider 100 includes a control mechanism 90, which permits the service provider to select what information elements stored in access device 102, including that derived from the configuration file 104, can be accessed by the user. In this way, the user is excluded from accessing information elements, which may be used to compromise the system security of the service provider.

Control mechanism 90 is preferably implemented in software, and may include one or more programs 93 for implementing functions in accordance with the present invention. Control mechanism 90 may be employed manually or automatically to flag certain information, such as designated web pages, to prevent user access. In manual mode, a person or persons at the service provider's location can designate files, web pages or other information that each end user either individually or as a group of end users will be denied access to from within the configuration file 104 of each user. In automatic mode, control mechanism 90 may scan for predesignated files, web pages, etc. which end users should not be able to access within their configuration file 104.

Control mechanism 90 may includes security measures 91 and designate a security code, level or index to sensitive information during a download sequence and may from time to time access the configuration files of end users to determine that these files were not illegally accessed. In one embodiment, portions 106 of configuration files may be designated in accordance with security risk, such that, access to certain designations of files is prohibited by the end user. These designations may be set manually or automatically, by the service provider. Advantageously, these settings may be remotely set or changed by the service provider from the service provider's location using a network management protocol such as, for example, a Simple Network Management Protocol (SNMP).

Service provider 100 may maintain a secured system, that is, access to service provider 100 is limited. In addition, information stored on service provider's systems may include information of a sensitive nature, which even end users need to be prevented from accessing.

Referring to FIG. 2 with continued reference to FIG. 1, service provider 100 (FIG. 1) retains control of which information elements can be revealed to an end user or subscriber; thereby enabling the service provider to maintain security over

the information elements which may enable the end user to compromise the service provider system's integrity if revealed to end users. Broadband access device 102 is programmed by service provider 100. Programs 106 in the configuration file 104 of device 102 may be designated at the time of download from the service provider or later designated/changed by the service provider by employing control mechanism 90. This feature of the present invention separates the files or components thereof into two groups, namely, service provider access only files 108 and end user access files 109. Device 102 may include a server 112, such as an HTML server, which is capable of displaying information included in files 109 to the end user. However, no access is provided to files 108, which have been designated by the service provider 100 to prevent access from the end user.

For example, an end user wishes to access the Internet through access device 102. The end user boots up a computer or other terminal device 110 but is unable to log onto his/her account maintained with service provider 100. The end user decides to run a diagnostic check of configuration file 104. The diagnostic feature is run form programs 106, but access to the output of the diagnostic tool is limited to only the information not designated for service provider access only 108. In this way, the system of service provider is securely maintained while the end user is still capable of performing needed tests and/or functions with device 102.

Referring to FIG. 3, a block/flow diagram is shown for a method for maintaining system security for a network service provider in accordance with one embodiment of the present invention. In block 202, a control mechanism is provided, preferably at the service provider's location, for remotely accessing end user network access devices. The control mechanism is preferably implemented as a software program for accessing and modifying the information of the access devices and designating portions thereof to prevent access by the end users. The control mechanism downloads information to an access device, initially (for example at the initial device configuration), and may provide levels of security or a security code for each component to limit access to the information depending on the security clearance that an end user may possess. The information stored is preferably a configuration file.

In block 204, the control mechanism or other means of the service provider can remotely access and modify the end user network devices to designate information stored on the access devices in accordance with the security codes or

levels or simply designate portions of the information as "off limits" to the end user. Remotely accessing the end user devices is preferably performed from a service provider's location. Advantageously, the information in an end user's configuration file may be accessed even after the information is downloaded. This permits the service provider the capability of accessing the configuration files to redesignate previously undesignated or designated information stored therein.

Different end users may have different levels of access depending on usage or clearance levels. Once designated, the end user is prevented from accessing the designated information on the end user's access device, in block 206.

In block 208, the service provider assigns security measures for the stored information to prevent access thereof by the end users. The service provider may employ security codes, security levels, passwords or other security measures to limit end user access to information stored on the network access device. The security codes or levels may be associated with the designated portions at or before initializing the access devices or after initializing the access devices.

Having described preferred embodiments for remote access control feature for limiting access to configuration file components (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in the particular embodiments of the invention disclosed which are within the scope and spirit of the invention as outlined by the appended claims. Having thus described the invention with the details and particularity required by the patent laws, what is claimed and desired protected by Letters Patent is set forth in the appended claims.